STATE OF WASHINGTON **NUMBER: 0030**
EMPLOYMENT SECURITY DEPARTMENT **PAGE: 1 OF 9**
POLICY AND PROCEDURE **DATE: 02/08/02**

Subject: SKIES Data Sharing, Data Disclosure and Security Administration

Purpose:

1) To provide direction for SKIES data sharing, data disclosure and administration of system security; 2) To define requirements for access to SKIES data; 3) To define roles and responsibilities for SKIES data sharing, disclosure and security administration; and 4) To assure compliance with applicable laws, rules and policies that govern SKIES data.

Applicability: This policy applies to all SKIES Data Recipients

Definitions:

"SKIES" (Services, Knowledge, and Information Exchange System) means the automated client tracking, accountability and reporting system used by the WorkSource service delivery system to support the delivery and management of employment and training services provided in the State of Washington under authority of the WorkForce Investment Act.

"WorkSource Partner" means an entity that is a party to a WorkSource Partnership Memorandum of Understanding and is performing WorkSource services pursuant to guidelines established by the WorkSource Executive Policy Council and includes that entity's officers, directors, officials, trustees, employees and/or agents including students and volunteers unless otherwise stated in the SKIES Data Sharing Contract.

"WDC" means one of the twelve Workforce Development Council entities in the State of Washington authorized under the Workforce Investment Act and includes that entity's officers, directors, officials, trustees, employees and/or agents including students and volunteers unless otherwise stated in the SKIES Data Sharing Contract.

"WIA Contractor" means an entity that has a contract to provide WorkForce Investment Act (WIA) employment and training services and includes the Contractor's officers, directors, officials, trustees, employees and/or agents including students and volunteers unless otherwise stated in the SKIES Data Sharing Contract.

"SKIES Data Recipient" means a WorkSource Partner (including ESD), WDC or WIA Contractor who is authorized to have access to or receives SKIES data.

"State SKIES Security Administrator" is an individual appointed by the ESD Assistant Commissioner for the Employment and Training Division to enforce the provisions of this policy and carry out other responsibilities identified below.

"WDC Security Administrator" is an individual and one or two alternates designated by the Workforce Development Area Director only in areas that choose the Decentralized Security Administration option described below. This individual authorizes user access in the local workforce development area and carries out other responsibilities identified below.

"System Administrator" is an individual and one or two alternates designated by the Workforce Development Area Director to maintain local table information in SKIES and carry out other responsibilities identified below. Every WDA is required to have a designated System Administrator.

“System Access Approver” is an individual designated by the Workforce Development Area Director in areas that choose the Centralized Security Option described below. Only System Access Approvers will have authority to submit a request to ESD Production Control to have a SKIES user added, deleted or modified.

Policy:

The Employment Security Department is responsible for protecting information in the SKIES system to assure it is held private and confidential consistent with RCW 50.13 and other applicable federal and state laws and rules identified below. SKIES Data Recipients shall limit access to the SKIES system and its data to those individuals whose currently assigned job duties result in a business need for access, and shall only share SKIES private and confidential information as specified in the following procedures and applicable SKIES Data Sharing Contract terms.

Procedure:

Minimum Requirements for SKIES Access

SKIES Data Recipients may have access to SKIES even though they may work in a satellite office or a remote location. The access will be predicated on the individual meeting the criteria, not on where they are located. Another method of access to SKIES would be through a contract for services that a local WDC or the state may have for WIA service delivery, evaluation and/or research purposes. Confidentiality of data shall be included as a condition of the SKIES Data Sharing contract. The following conditions must be met for all SKIES users:

1. User’s agency or organization is a recognized WorkSource Partner Agency as evidenced by a signed WorkSource Memorandum of Understanding with the local Workforce Development Council (WDC) or has a contract with the WDC or Employment Security Department to provide WIA services and has access, disclosure and security requirements written into a SKIES Data Sharing Contract;
2. User’s agency or organization has a signed SKIES data sharing contract with ESD;
3. User has completed SKIES training;
4. And, User has signed the SKIES Notice of Non-disclosure.

“Opt Out” Requirements

The “Opt Out” provisions of RCW 50.13.060 (11) (b) apply to any agency or organization that enters client information into the SKIES system. As an alternative to entering client data into SKIES for clients who choose to exercise the “opt out” option, other methods including “paper” records may be used. When “paper” records are used by a non-ESD SKIES Data Recipient for the purpose of honoring an “opt out” request, the paper record may be shared with an ESD employee who shall enter the record into the SKIES system as necessary to meet federal and state reporting requirements.

SKIES Data Sharing Contracts

Each SKIES Data Recipient is required to have a “SKIES Data Sharing Contract” with ESD before access will be granted to its employees. This data sharing contract must specify the business case for access to the SKIES system, and must include all of the provisions noted below.

General Provisions to be included in all SKIES Data Sharing Contracts

The ESD SKIES Data Sharing Contract Boilerplate must be used for all SKIES data sharing contracts between SKIES Data Recipient(s) and ESD. Contracts are subject to approval by the State SKIES Security Administrator and the ESD Contracts Office in accordance with ESD Policy #0029. The State SKIES Security Administrator shall obtain approval and signature of the owning Division's designated Data Owner(s) before approving the Data Sharing Contract.

Data Sharing Contract Requirements for WDAs with Decentralized Security Administration

Data Sharing Contracts for WDAs electing decentralized security administration (see below) shall include a special clause delegating authority and responsibility for SKIES application security administration including authorization for user access to the designated WDC Security Administrator. Subject to the terms and conditions of the SKIES Data Sharing Contract, the WDA Security Administrator is authorized to grant SKIES Data Recipient access to the SKIES on-line application. This authority shall include the ability to create and manage user access to SKIES, and access to confidential SKIES data.

1. The WDA Security Administrator shall be responsible for maintaining auditable records to demonstrate that all documentation requirements are met for each SKIES user prior to granting access to the SKIES system.
2. The WDA Director shall appoint the WDA Security Administrator. The WDC shall comply with ESD policies for data security and disclosure including classification and accompanying requirements for use of data.
3. ESD's Security Administrator, State or External Auditors and Internal Auditors of ESD shall have the right at any time to audit any and all elements of SKIES security administration and data disclosure at the Workforce Development Council and/or at any SKIES Data Recipient site.
4. Any violations of the SKIES Data Sharing Contract may result in revoking of access to SKIES data including Unemployment Insurance and/or Employment and Training data within SKIES. Any Data Sharing Contract violation review, decision and communication of a revocation action will occur at the direction of the State SKIES Security Administrator in accordance with the Termination of Access provision of the SKIES Data Sharing Contract.

Requests for Access to SKIES Records

All requests from the public or subpoenas received by SKIES Data Recipient for access to SKIES records in accordance with RCW 42.17 or RCW 50.13 shall be immediately reported to the State SKIES Security Administrator. The SKIES Data Recipient shall instruct the requestor to submit the request in writing to:

Employment Security Department
Records Disclosure Unit
PO Box 9046
Olympia, WA 98507

The request will be processed by the ESD Records Disclosure Unit in accordance with published rules for release of information.

User Access Profiles

The appropriate user access profile is to be assigned to each SKIES user based on the individual's business needs. The profiles are as follows:

Staff

For use by WIA program direct-service staff for case management and service tracking. Allows full insert, update and delete access to most fields.

Read only

For staff who need "view" access only. Does not allow insert, update or delete access.

Reception

For use by front-desk staff. Access is limited to simple initial data entry, address changes, and correspondence.

Correspondence

Allows access to create correspondence templates.

IT Staff

For local table maintenance.

Security Administration

For use by SKIES Security Administrators to add and maintain users in WDAs electing the Decentralized Security Option.

System Maintenance

For business analysts at ESD who will be responsible for maintenance of "list of values" that are used statewide and for other statewide ESD administrative maintenance tasks (ESD Employment and Training Division Only).

State SKIES Security Administrator

The State (ESD) SKIES Security Administrator, appointed by the Assistant Commissioner for the Employment and Training Division, has authority to grant "Security Administration" profile access and to authorize SKIES access to ESD Central Office staff. The State SKIES Security Administrator also has the following responsibilities:

1. Enforce the provisions of this policy at the local and State level
2. Authorize access to the SKIES Data Warehouse in accordance with ESD Policy #0029. The State SKIES Security Administrator shall obtain approval and signature of the owning Division's designated Data Owner(s) before approving Data Warehouse access.
3. Monitor local level security administration and data sharing/disclosure requirements
4. General local level oversight, support and technical assistance on security, data sharing and disclosure issues
5. Participate in SKIES system design changes.

WDA Security Administration Options

There are two optional methods for administering SKIES security at the local WDA level. These options are described below. The Director of each Workforce Development Area will notify the State SKIES Security Administrator in writing of which option will be used to administer security.

Option 1 - Decentralized Security Administration

The WDC identifies a WDC Security Administrator who is responsible for managing system access and security. The state role for areas choosing this option is limited to monitoring and auditing of user access, data sharing and policy oversight as well as providing technical assistance to the local WDAs.

WDC Security Administrator (Option 1 Only)

The Workforce Development Area Director shall appoint one WDC Security Administrator and one or two alternates in writing. The WDA Security Administrator will have sole responsibility for authorizing "user access" to the SKIES on-line application for all authorized system users within the WDA, including ESD employees as well as non-ESD agency employees. The WDA Security Administrator shall also have the following responsibilities:

1. Assign user logon Ids and remove users from the system,
2. Assure that a valid and current SKIES Data Sharing Contract with the Employment Security Department (ESD) is in place for each agency or organization that employs SKIES users,
3. Develop a system to assure that SKIES access is immediately revoked for users at such time that the data sharing contract for his/her agency or organization expires or when the terms of the SKIES Data Sharing Contract have been breached,
4. Signed Non Disclosure statements are on file for all users and available for audit,
5. Certification of SKIES training completion is on file for all users and available for audit,
6. Assure that access is granted only to users who work for an agency or organization that is party to a WorkSource Memorandum of Agreement (WorkSource Partner) or is a WDC or ESD contractor for services under the Workforce Investment Act and has a valid and current SKIES Data Sharing Contract with ESD,
7. Assures that SKIES user accounts are deactivated immediately when the user is no longer employed with the WorkSource partner or WDC contractor,
8. Assure that the type of access granted (user profile) is justified based on business needs and is approved by the user's supervisor,
9. Record Keeping is sufficient to allow for monitoring and auditing,
10. Verification of employment status for ESD employees,
11. Ensure compliance with all applicable statutes, laws, rules and policies related to data sharing, disclosure and SKIES security administration,
12. Assure effective security practices are followed including: only one user account per staff, no sharing of userids or passwords, and use of system data only for intended business purposes.
13. Provides local level oversight, support and technical assistance relating to data sharing, disclosure and security administration,
14. Enforcement of the provisions of this policy at the local level,
15. Reporting of system abuse and security breaches to the State SKIES Security Administrator, and
16. Assures that "Opt Out" requirements under RCW 50.13.060 (11) (b) are properly administered at the local level.

Option 2 - Centralized Security Administration

The State has most of the responsibility for system administration, with limited local participation in the system security process.

Designation of System Access Approvers

Each WDA that adopts the Centralized Security option will designate “System Access Approvers” who will have authority to submit a request to have a SKIES user added, deleted or modified (See “Option 2 Procedure to Add/Delete/Modify User Access” below). Only designated System Access Approvers will be allowed to submit SKIES user requests for both ESD and non-ESD agency employees within the WDA. Upon submitting a request to add a new user, the System Access Approver will certify that the following conditions have been met: 1) the user has completed required training, 2) the user profile requested is appropriate and based on business needs, and 3) the new user has signed a SKIES Notice of Non-Disclosure which is on file and available for audit. System Access Approvers would generally be limited to administrators and supervisory staff.

ESD responsibilities – Centralized Security Administration

The ESD Production Control Unit shall have the following responsibilities for ESD and non-ESD agency employees in WDAs choosing the Centralized Security option:

1. Process local requests for user access
2. Assign user logon Ids and remove users from the system on receipt of complete and duly authorized requests from System Access Approvers
3. Assure that a valid SKIES Data Sharing Contract is in place for each agency or organization that employs SKIES users
4. Assure that SKIES access is immediately revoked for users at such time that the data sharing Contract for his/her agency or organization expires
5. Assure that signed Non Disclosure statements are on file for all users and available for audit
6. Assure that Access is granted only to users who work for an agency or organization that is party to a WorkSource Memorandum of Agreement (WorkSource Partner) or is a WDC or ESD contractor for services under the Workforce Investment Act
7. Assure that the type of access granted (user profile) is justified and is approved by the user’s supervisor
8. Verify employment status for ESD employees

The State SKIES Security Administrator shall be responsible for ensuring compliance with all applicable statutes, laws, rules and policies related to data sharing, disclosure and SKIES security administration.

WDA responsibilities – Centralized Security Administration

1. Designate System Access Approvers who have authority to authorize user access to SKIES application data
2. Assure that all users complete appropriate SKIES training
3. Provide local level oversight, support and technical assistance relating to data sharing and disclosure
4. Enforce security rules and policy at the local level
5. Report system abuse and security breaches to the State SKIES Security Administrator
6. Assure that “Opt Out” requirements under RCW 50.13.060 (11) (b) are properly administered at the local level
7. Notify ESD Production Control when users need to be deactivated, using the on-line request form (See “Option 2 Procedure to Add/Delete/Modify User Access” below)

Option 2 Procedure to Add/Delete/Modify User Access

ESD Production Control will provide an on-line password protected request form that can be accessed by any designated Authorized Approver. This on-line form will be used to transmit all information needed to process a request to add, delete or modify a SKIES user. The Production Control unit at ESD will process these requests. Each request will be checked to verify that all conditions for SKIES access have been satisfied. Upon approval of the request, the user will be added, deleted or modified in SKIES as requested, and the Authorized Approver and user will receive notification of the action taken.

Monitoring and Audit

The SKIES system, its data, and security administration procedures at the local level shall be subject to audit by ESD Internal Audit and monitoring by duly authorized representatives of ESD and Office of the State Auditor.

Sanctions

Violation of this policy may result in revocation of access to the SKIES system in accordance with the Termination of Access provision of the SKIES Data Sharing Contract. The misuse or unauthorized release of records or information considered private and confidential by any person or organization shall subject an individual or organization to a civil penalty of five thousand dollars and other applicable sanctions under state and federal law.

Designation of System Administrator

The Workforce Development Area Director shall appoint in writing one System Administrator and one or two alternates. System Administrator responsibilities include:

1. Add and update local table information
2. Maintain Providers list
3. Maintain local office information
4. Maintain correspondence templates
5. Maintain Test Administration function
6. Identify and report local system and performance issues

System Administration Training

The Employment and Training Division will provide training and support for administration of SKIES at the local level. SKIES System and Security Administration training will include:

1. Office Maintenance
2. Table Maintenance
3. Staff Maintenance
4. Correspondence Maintenance
5. Test Administration
6. Provider List maintenance
7. Security Administration, Data Sharing and Data Disclosure Requirements

SKIES User Support

Support for SKIES users is provided through a three-tiered approach. This assures the best customer service and the effective use of available resources. The following is an overview of this three-tiered system.

Level One Support

a. An on-line SKIES Knowledge Base (available through the SKIES web site, along with other useful SKIES resources), enables the front-end customer access to a wide variety of customer service responses and answers to user questions.
b. A SKIES Discussion Board facilitates discussion among users. The Discussion Board provides useful up-to-date on-line information and encourages sharing of experiences. It is available through the SKIES web site.
c. Each WDA will designate a local SKIES User Support Coordinator(s) who is available to customers within the WDA and who is fully SKIES knowledgeable. The hours of availability are a local decision. Users are encouraged to seek assistance from the local Support Coordinator prior to contacting the SKIES help desk.

Level Two – for problems unresolved through Level One

a. The SKIES Help Desk is available Monday through Friday from 8:00 am to 5:00 pm. A SKIES Help Desk phone line, (360) 438-4690, will be available to customers needing to contact the Help Desk.
b. The SKIES Help Desk phone line is available to provide immediate access to Help Desk staff. In cases where immediate help is necessary, and Help Desk staff are unable to immediately resolve the problem, staff will refer the request to the appropriate expert who will be responsible for making prompt follow-up contact with the customer. All customer questions will be tracked through Remedy (an on-line customer tracking database), assuring full records and reporting capacity and assuring each request is properly processed.

Level Three – for problems unresolved through Level Two

a. A panel of **SKIES experts** will be available to respond to customer queries that have not been resolved through Levels One and Two. Remedy will be used to route customer requests to the appropriate expert.

b. Experts are also available by phone for immediate consultation with customers as needed.

Local SKIES User Support Coordinator Roles and Responsibilities

The Local SKIES User Support Coordinator assures the availability of localized user support for the SKIES application. Responsibilities may include:

a. Has expert knowledge of the SKIES application and the local area policies, procedures and business processes related to SKIES

b. Assures availability of knowledgeable on-site assistance in each CDC or Affiliated site office

c. Provides clarification on business issues or problems related to implementation of SKIES at the local level

d. Determines which problems are best resolved at the local level, and which need to be elevated to the state level

e. Acts as liaison with state help desk to assure good communication and coordination of user support

f. Collects information about recommended revisions for consideration for future versions

Related Laws, Rules and Policies:

SKIES Data Recipients must ensure that data is used consistent with these applicable privacy laws:

ESD Policies and Procedures #0029 – On-Line or Bulk Data/Information Sharing
RCW 50.13.060 Records and Information – Privacy and Confidentiality
RCW 42.17.260 Disclosure
Workforce Investment Act
Governor’s Executive Order 003 on Public Record Privacy Protection
Privacy Act of 1974
Social Security Act

Direct Inquiries to:

Joe Racek, State SKIES Security Administrator, Employment Security Department, (360) 438-4100.